JEDI

Secure Infrastructure Management for the Enterprise

PRéCis Overview

Capt Ryan Durante
JEDI Program Manager
AFRL/IFEB
Comm: 315-330-7657, DSN: 587
email:

Agenda

- What is PRéCis?
- PRéCis Architecture
  - Agents
  - Server
  - What does PRéCis do
    - Audit Management
    - Host based intrusion detection
    - Damage Assessment
    - Countermeasures
  - User Interfaces
- Summary
- Questions/Discussion

What is PRéCis

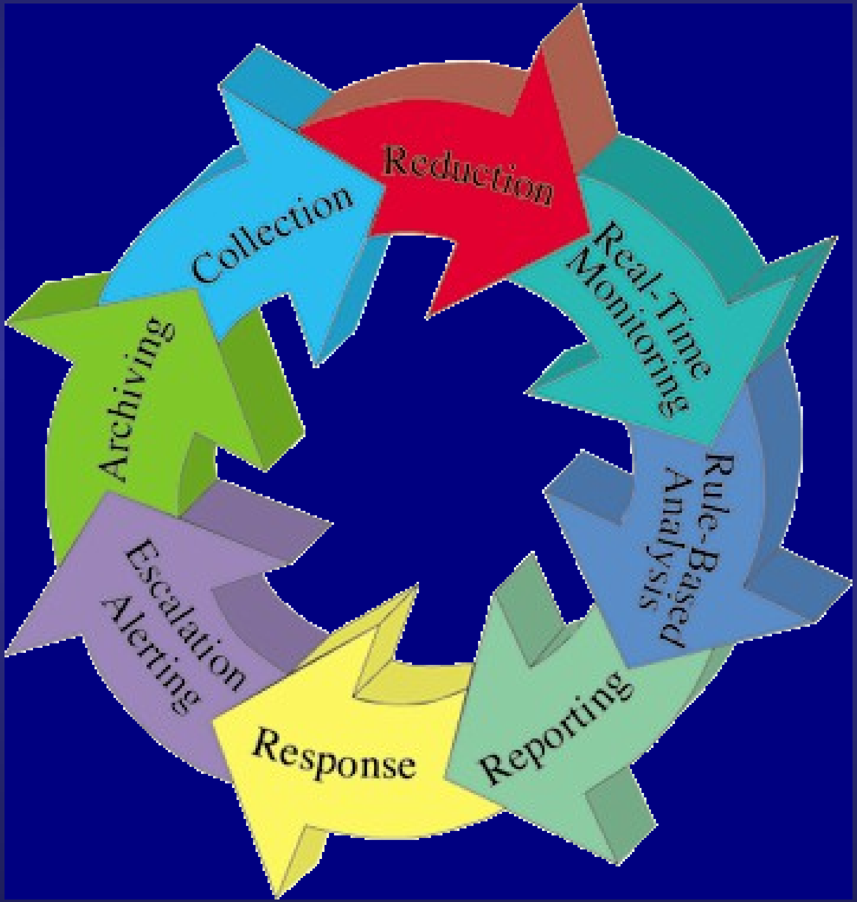
PRéCis is a toolkit that automates all aspects of audit processing in a network environment.

The suite of automated tools provides you with the flexibility to implement a turnkey security policy or one that can be tailored to your own specific security policy.

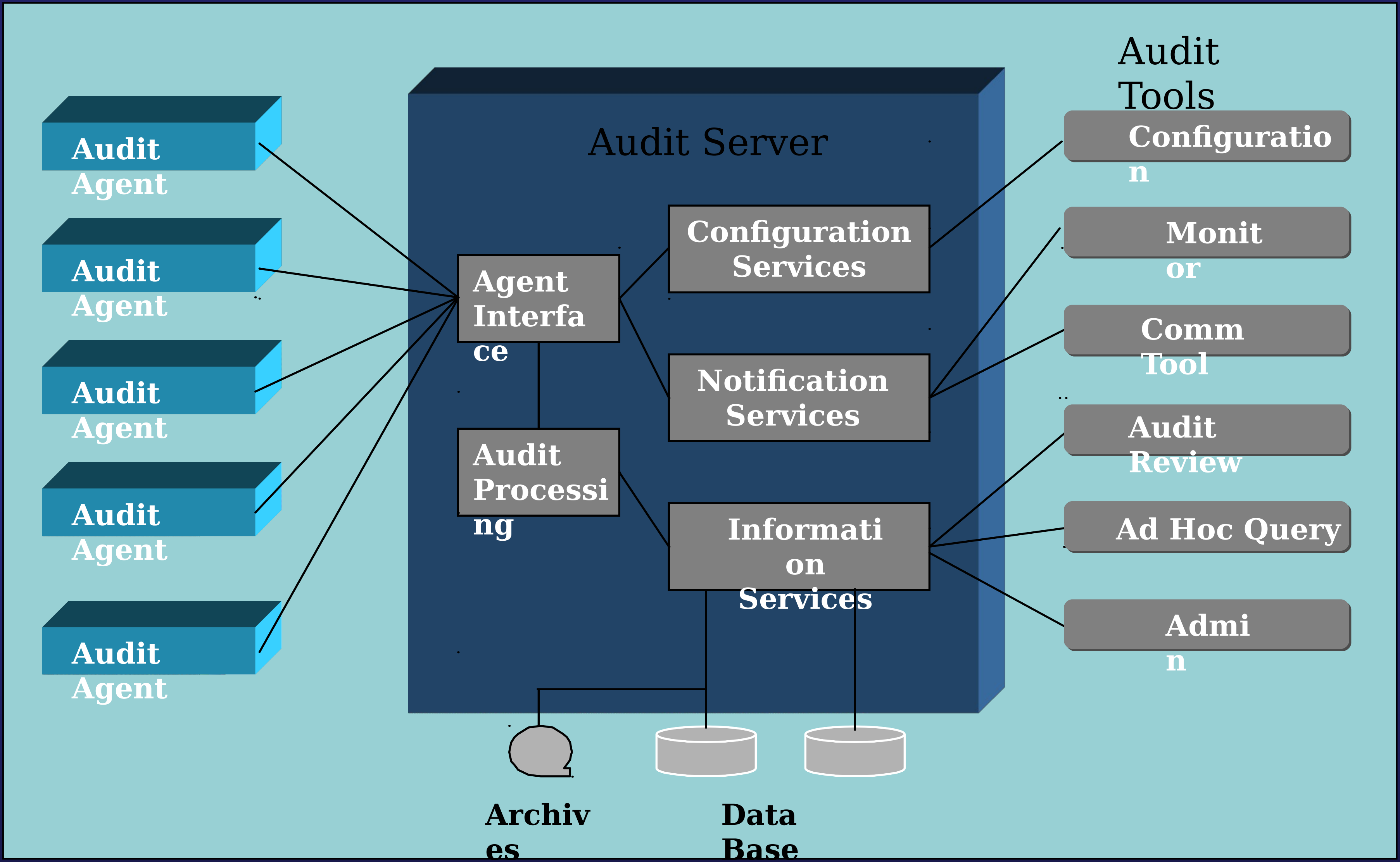
PRéCis will be available un-bundled from the

What is PRéCis (continued)

- Audit Collection
  - Reduction
  - Archiving
- Real-Time Monitoring
  - Rule-based Analysis
  - Reporting
  - Response
  - Escalation Alerting



PRéCis Architecture



PRéCis Agents

Audit Agent

Audit Agent

Audit Agent

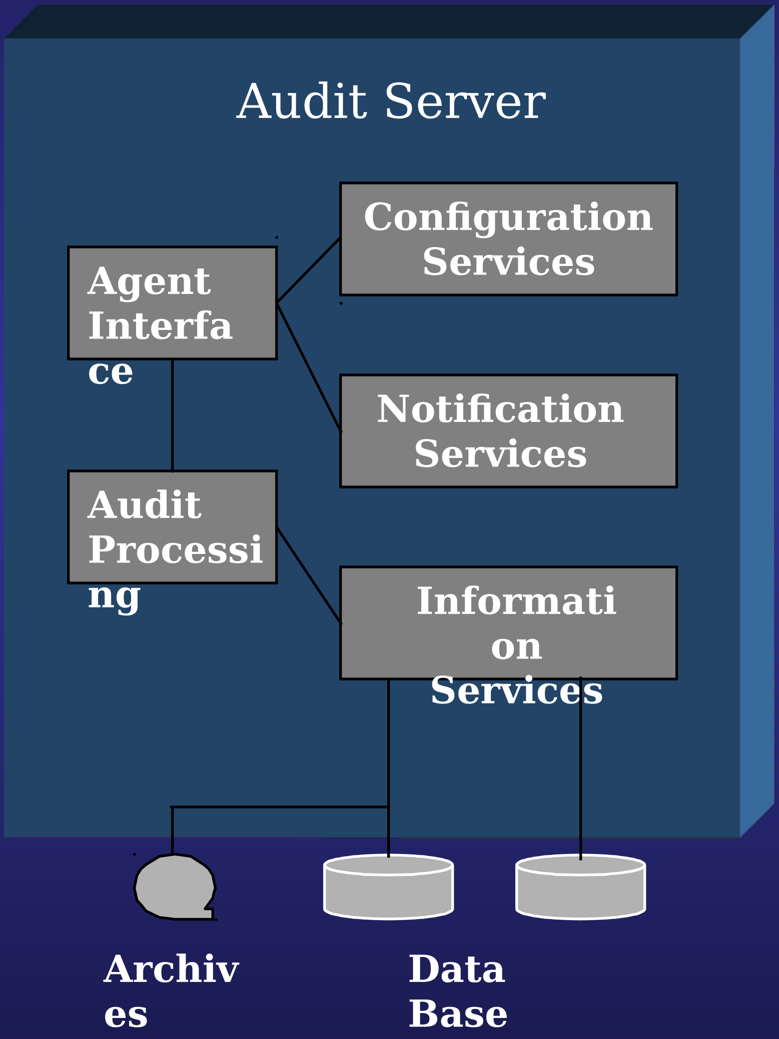
Audit Agent

Audit Agent

- Reside on audit source nodes in a network
  - Run on NT, Win2K, Solaris
  - Level 0 (Basic Agents)
  - Level 1 (Audit Collection Server (ACS) Agents)
- Capture Native Audits from Operating System or applications.
- Convert to Normalized Representation
  - Filter for critical events
  - Reduce quantity of audits transmitted
  - Native audits bulked to Server during off-peak

PRéCis Server

- Supports an Agent/Manager interface
  - Audit collection
  - Agent control
  - Agent configuration
- Provides audit processing for data base load and archiving of native audits



- Maintains a centralized audit data repository
  - Normalized
  - Native
  - Virtual Storage
- Client/Server interface with Audit Tools
- Monitoring

What does PRéCis Do?

Audit Management

Audit Management: the ability to store, retrieve and manipulate audit data (and other supporting data) for the purpose of reporting or performing historical analysis.

PRéCis Provides:

- evidence needed to support damage assessments and possible prosecution
- permanent record of events
- sufficient level of auditing to occur
- automated handling of files

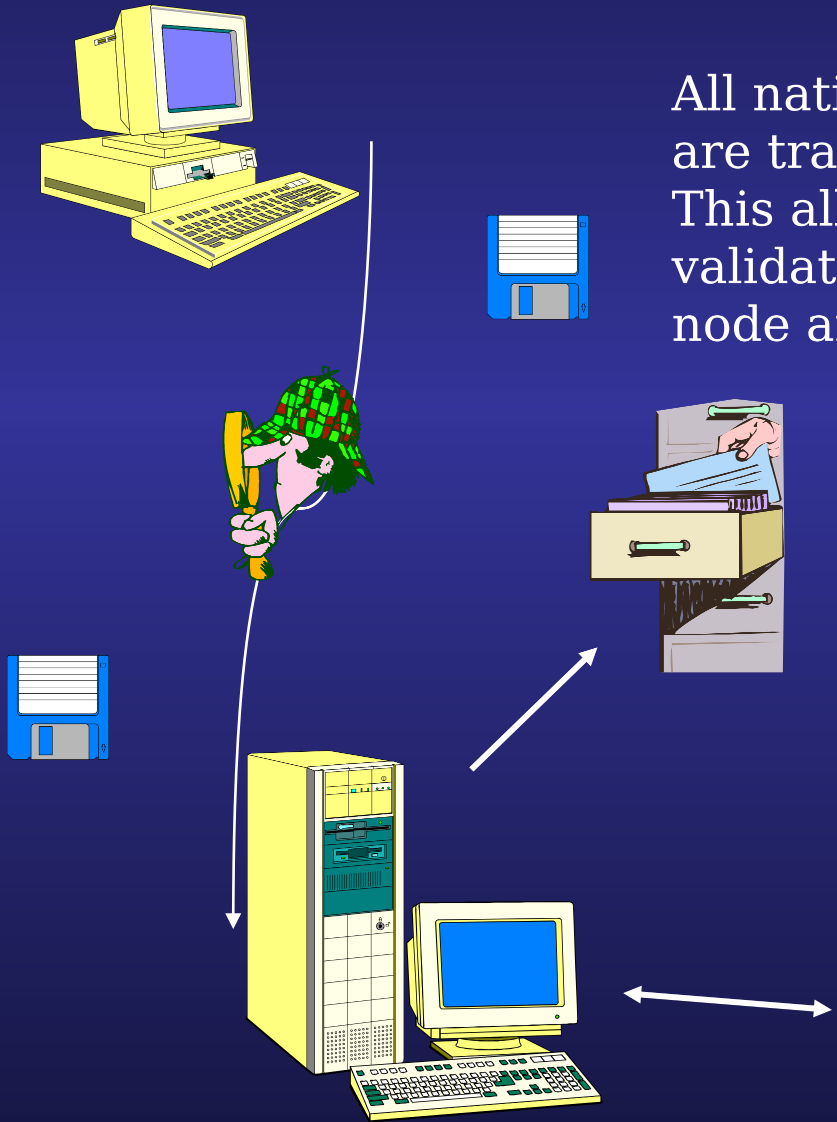
Audit Management (continued)

PRéCis comes with a flexible, configurable and easy to use archiving subsystem. The system completely automates all aspects of data storage and retrieval to the media of choice.

PRéCis Advantages:

- allows site to specify archiving options, including compression
- flexible command execution allows site specific devices to be used
- the archive process is internally audited
- temporary online archive is available for rapid retrieval

Audit Management (continued)



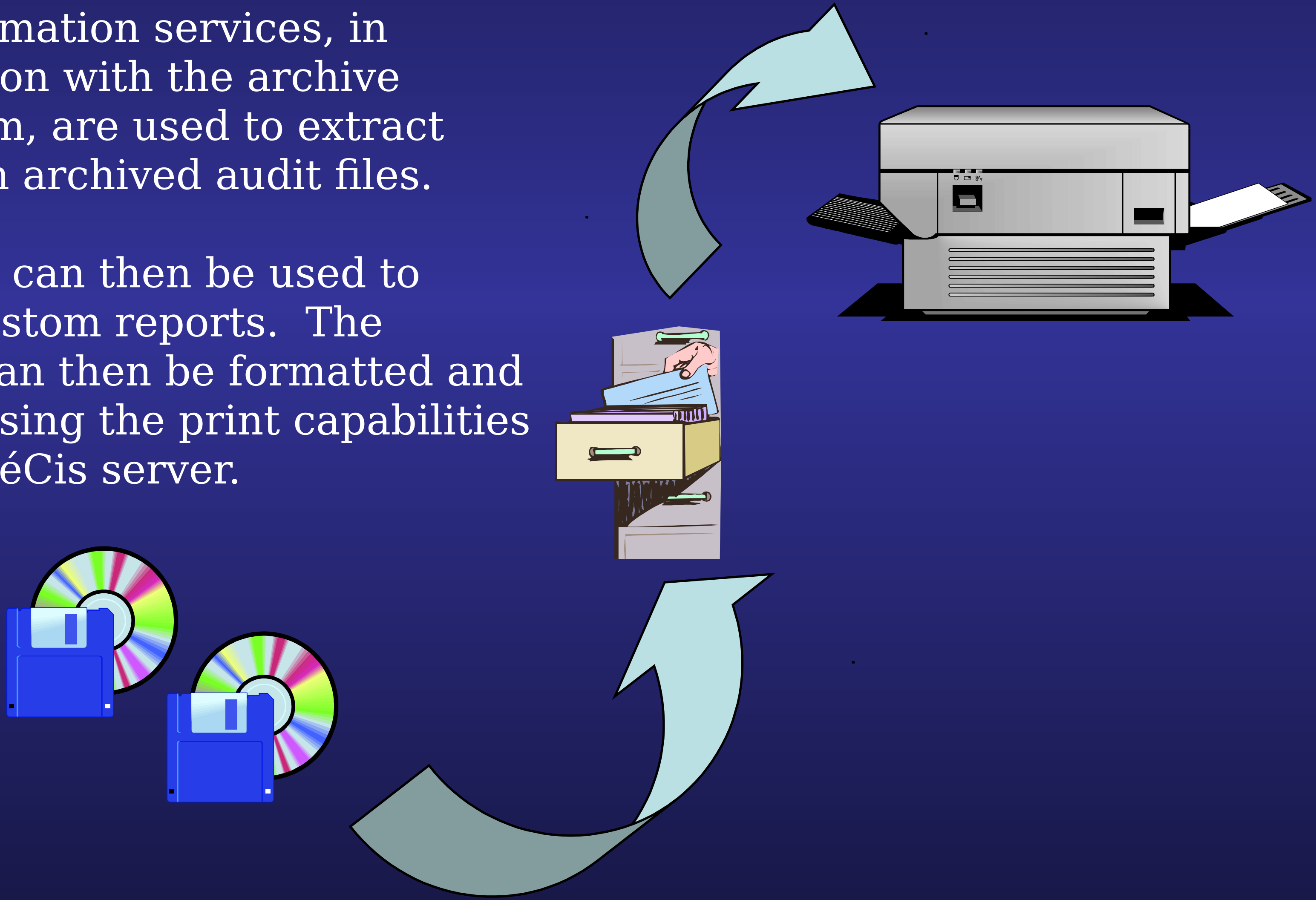
All native audit files that are being processed are tracked within the relational database. This allows the agent process to perform a validated file transfer between the monitored node and the PRéCis server.

Once the files are transferred to the server, the archive subsystem executes site configurable commands to move the files to storage media.

Audit Management (continued)

The information services, in conjunction with the archive subsystem, are used to extract data from archived audit files.

This data can then be used to create custom reports. The reports can then be formatted and printed using the print capabilities of the PRéCis server.



Host-based Intrusion Detection

Host-based ID: the analysis of user activities on a computer system to detect malicious behavior or misuse. Cross platform analysis can be performed by correlating data from all systems on a LAN.

PRéCis Provides:

- internal threat detection as well as external
- detection regardless of IPSEC
- misuse and malicious detection
- site specific implementation

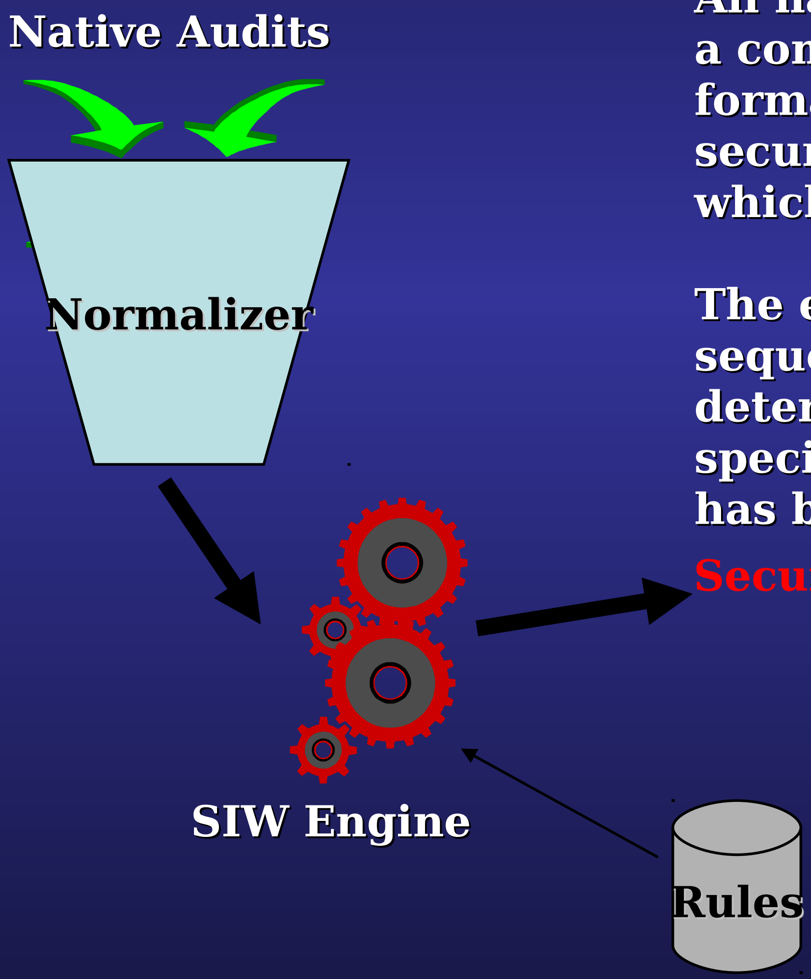
Host-based Intrusion Detection (continued)

PRéCis performs real-time host based intrusion detection using a indication and warning technology that determines potential misuses and malicious behavior.

Advantages:

- analysis is based on normalized data from multiple sources
- default or site specific rules are loaded at runtime
- allows site specific security policy to be implemented and monitored

Host-based Intrusion Detection (continued)



Native Audits

Normalizer

SIW Engine

Rules

All native audit events are converted to a common format (normalized) and fed into the security indication and warning engine which resides on the PRéCis server.

The engine allows multiple, non-sequenced events to be analyzed to determine if an alert threshold, as specified by the site's security policy, has been exceeded.

Security Policy Violation Alert

Damage Assessment

Damage Assessment: the ability to determine what information was compromised and to what extent. This includes answers to who, when, where and how.

PRéCis Provides:

- reports based on site specified data analysis
- evidence of lost or compromised data
- feedback on weaknesses and security holes

Damage Assessment (continued)

PRéCis simplifies the security officer’s task by providing a standardized audit format derived from heterogeneous native audit data.

This normalized format and data reduction greatly reduces the volume of audit data for review. Normalized audit records are linked back to the original native records to facilitate in-depth analysis.

Advantages:

- reduction of data
- heterogeneous data displayed in a homogeneous format
- site defined report formats

Countermeasures

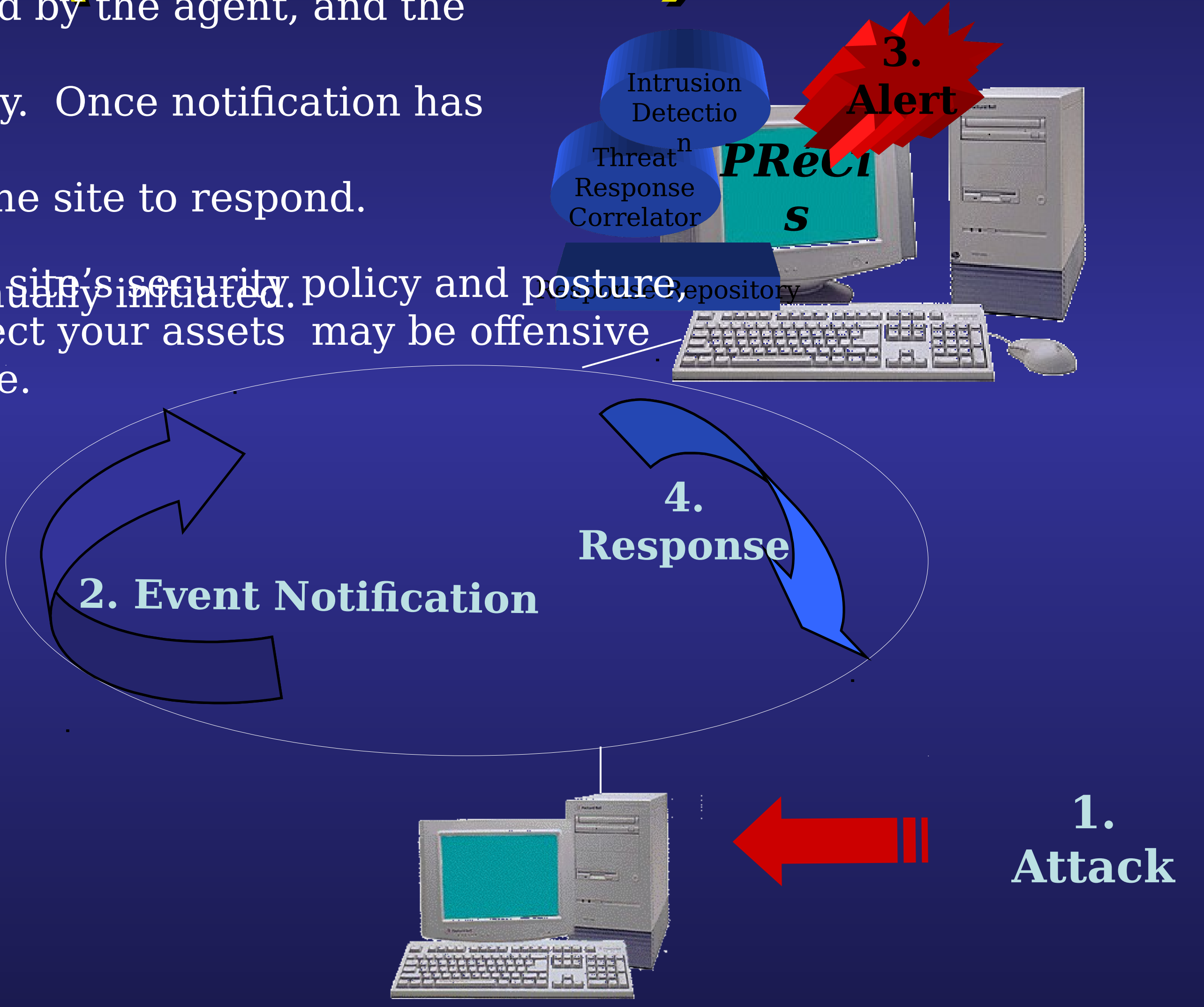
Countermeasure: An action or group of actions taken, either manually or automatically, to thwart an attack, track suspicious user and/or counter the actions of an individual.

PRéCis Advantages:

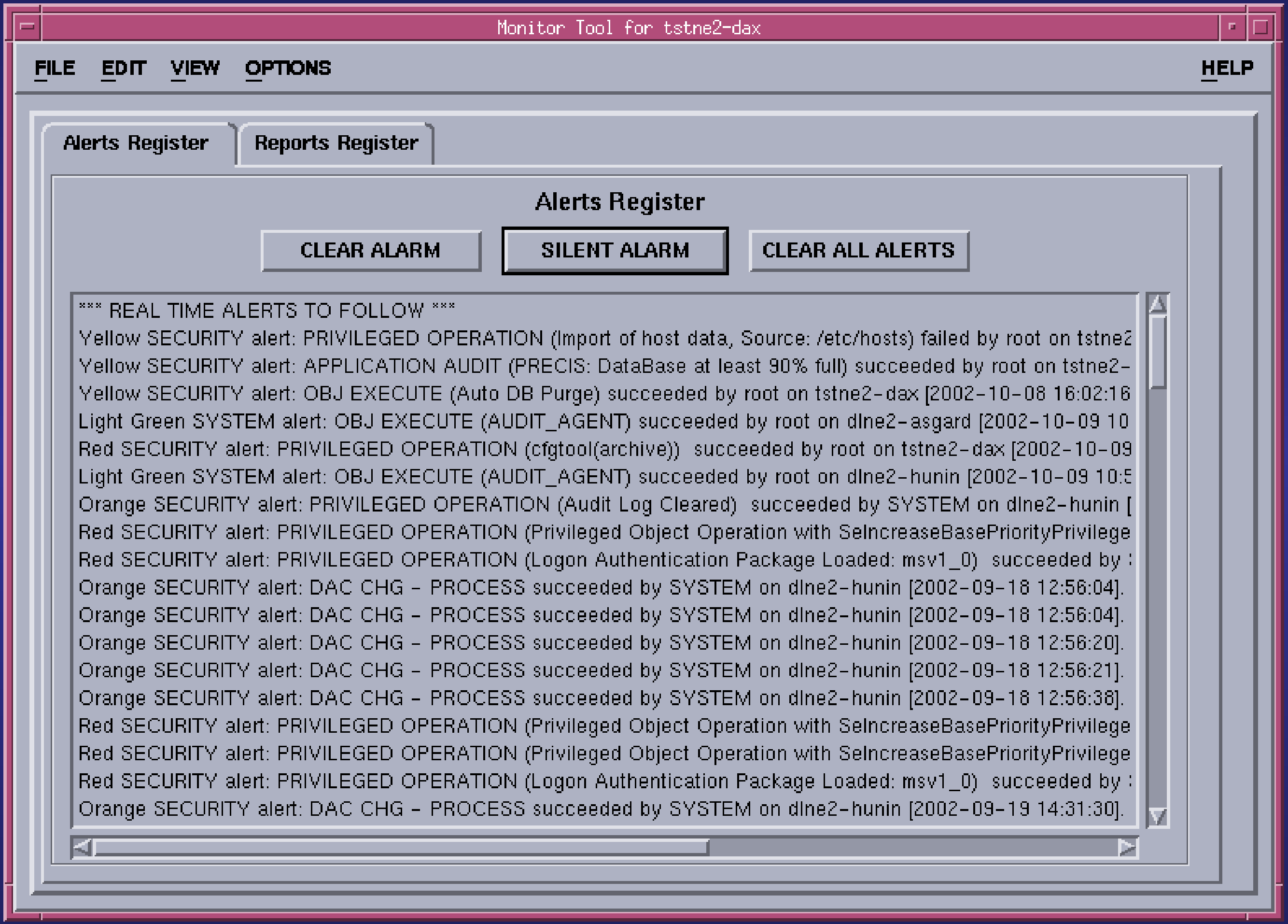
- ability to terminate access method
- potentially can prevent attacks from completing
- responses can be determined by site

Countermeasures (continued)

- An event is detected by the agent, and the server is notified accordingly. Once notification has been received, it is up to the site to respond. Responses may be automatic or manually initiated.
- Depending on your site's security policy and posture, the response to protect your assets may be offensive or defensive in nature.
- A standard set of responses is provided with PRéCis along with an easy to use API.



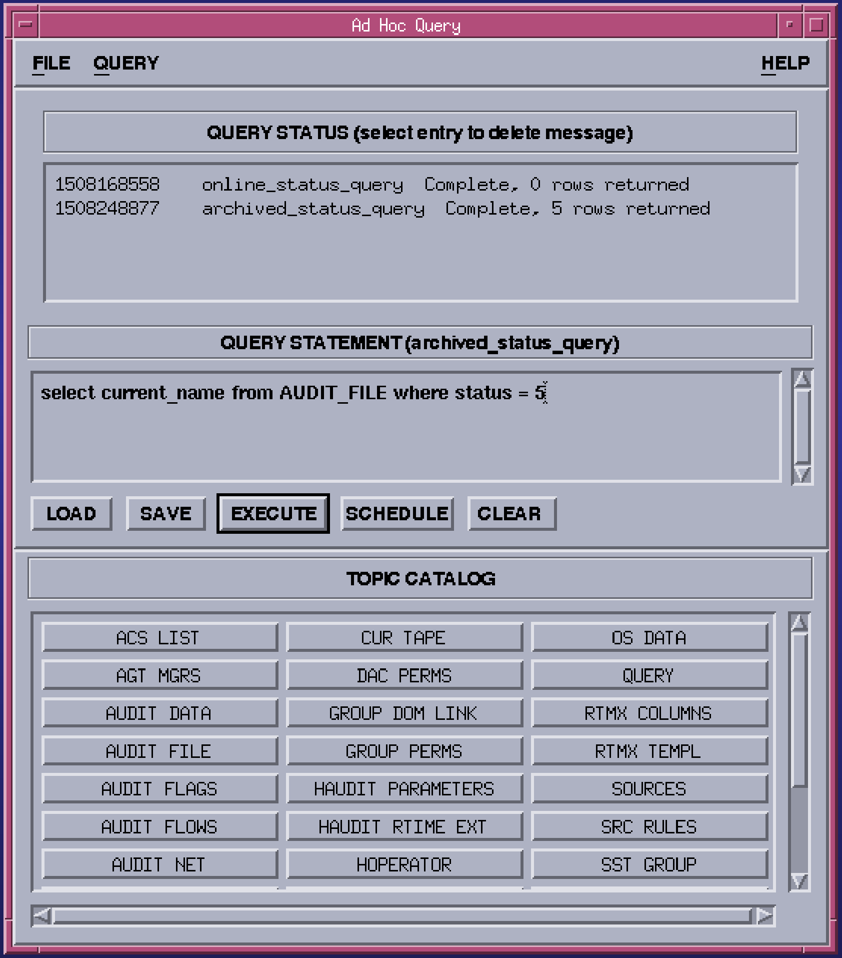
PRéCis User Interfaces



```
*** REAL TIME ALERTS TO FOLLOW ***
Yellow SECURITY alert: PRIVILEGED OPERATION (Import of host data, Source: /etc/hosts) failed by root on tstne2
Yellow SECURITY alert: APPLICATION AUDIT (PRECIS: DataBase at least 90% full) succeeded by root on tstne2-
Yellow SECURITY alert: OBJ EXECUTE (Auto DB Purge) succeeded by root on tstne2-dax [2002-10-08 16:02:16
Light Green SYSTEM alert: OBJ EXECUTE (AUDIT_AGENT) succeeded by root on dlne2-asgard [2002-10-09 10
Red SECURITY alert: PRIVILEGED OPERATION (cfgtool(archive))  succeeded by root on tstne2-dax [2002-10-09
Light Green SYSTEM alert: OBJ EXECUTE (AUDIT_AGENT) succeeded by root on dlne2-hunin [2002-10-09 10:5
Orange SECURITY alert: PRIVILEGED OPERATION (Audit Log Cleared)  succeeded by SYSTEM on dlne2-hunin [
Red SECURITY alert: PRIVILEGED OPERATION (Privileged Object Operation with SeIncreaseBasePriorityPrivilege
Red SECURITY alert: PRIVILEGED OPERATION (Logon Authentication Package Loaded: msv1_0)  succeeded by :
Orange SECURITY alert: DAC CHG - PROCESS succeeded by SYSTEM on dlne2-hunin [2002-09-18 12:56:04].
Orange SECURITY alert: DAC CHG - PROCESS succeeded by SYSTEM on dlne2-hunin [2002-09-18 12:56:04].
Orange SECURITY alert: DAC CHG - PROCESS succeeded by SYSTEM on dlne2-hunin [2002-09-18 12:56:20].
Orange SECURITY alert: DAC CHG - PROCESS succeeded by SYSTEM on dlne2-hunin [2002-09-18 12:56:21].
Orange SECURITY alert: DAC CHG - PROCESS succeeded by SYSTEM on dlne2-hunin [2002-09-18 12:56:38].
Red SECURITY alert: PRIVILEGED OPERATION (Privileged Object Operation with SeIncreaseBasePriorityPrivilege
Red SECURITY alert: PRIVILEGED OPERATION (Privileged Object Operation with SeIncreaseBasePriorityPrivilege
Red SECURITY alert: PRIVILEGED OPERATION (Logon Authentication Package Loaded: msv1_0)  succeeded by :
Orange SECURITY alert: DAC CHG - PROCESS succeeded by SYSTEM on dlne2-hunin [2002-09-19 14:31:30].
```

The Real-Time Monitor tool displays the main GUI that provides a way t review audits from a selected source in near-real time

PRéCis User Interfaces (continued)

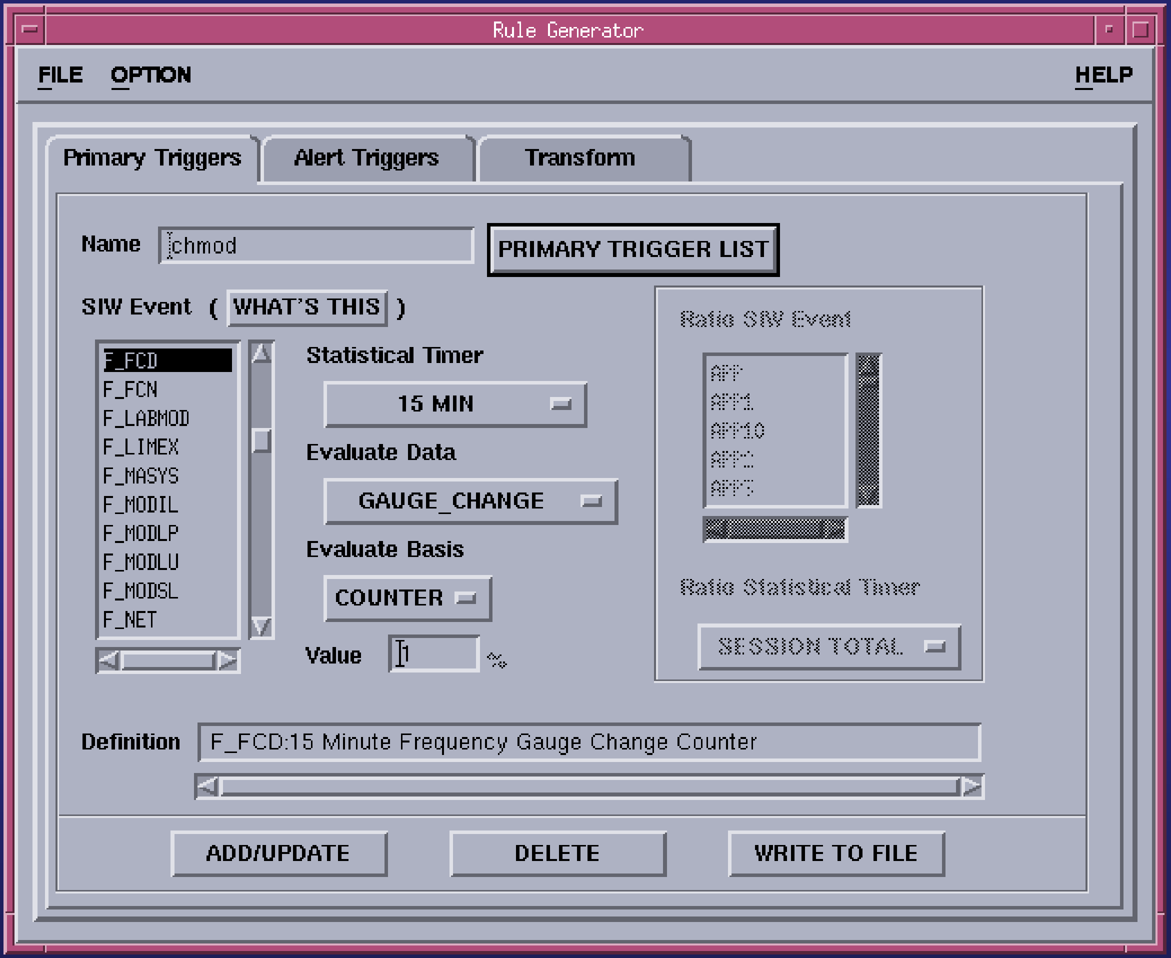


```
1508168558    online_status_query   Complete, 0 rows returned
1508248877    archived_status_query   Complete, 5 rows returned
```

```
select current_name from AUDIT_FILE where status = 5
```

The Ad Hoc Query Tool allows you to formulate and execute queries for normalized audits and other information in the database using SQL.

PRéCis User Interfaces (continued)



Name: chmod

SIW Event (WHAT'S THIS)

F_FCD
F_FCN
F_LABMOD
F_LIMEX
F_MASYS
F_MODIL
F_MODLP
F_MODLU
F_MODSL
F_NET

Statistical Timer: 15 MIN

Evaluate Data: GAUGE_CHANGE

Evaluate Basis: COUNTER

Value: 1 %

Ratio SIW Event

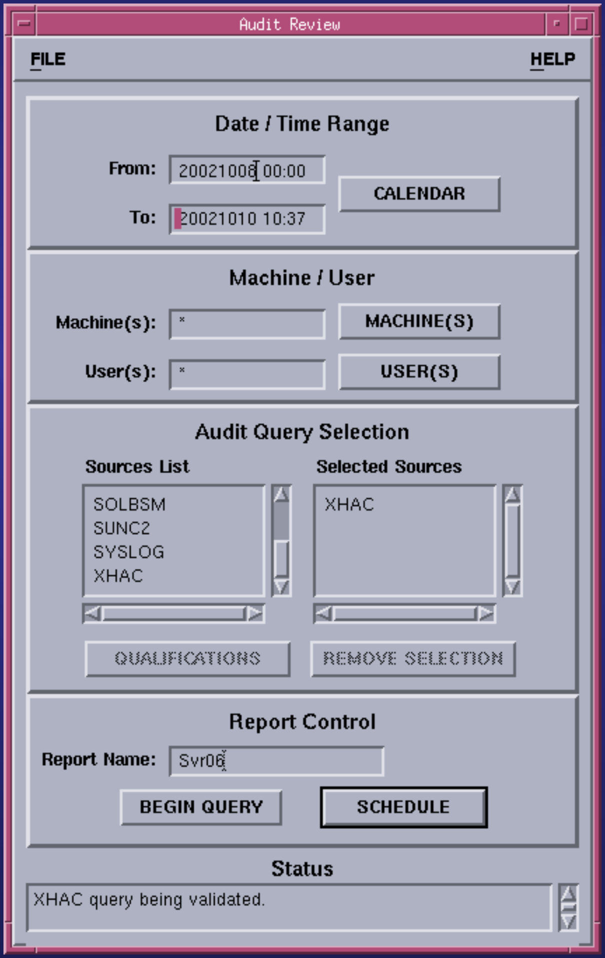
APP
APP1
APP10
APP2
APP3

Ratio Statistical Timer: SESSION TOTAL

Definition: F_FCD:15 Minute Frequency Gauge Change Counter

The Security Indications and Warnings (SIW) (Rule) Generator Tool is designed to alert you when events occur.

PRéCis User Interfaces (continued)



From: 20021008 00:00

To: 20021010 10:37

Machine(s): *

User(s): *

Sources List: SOLBSM, SUNC2, SYSLOG, XHAC

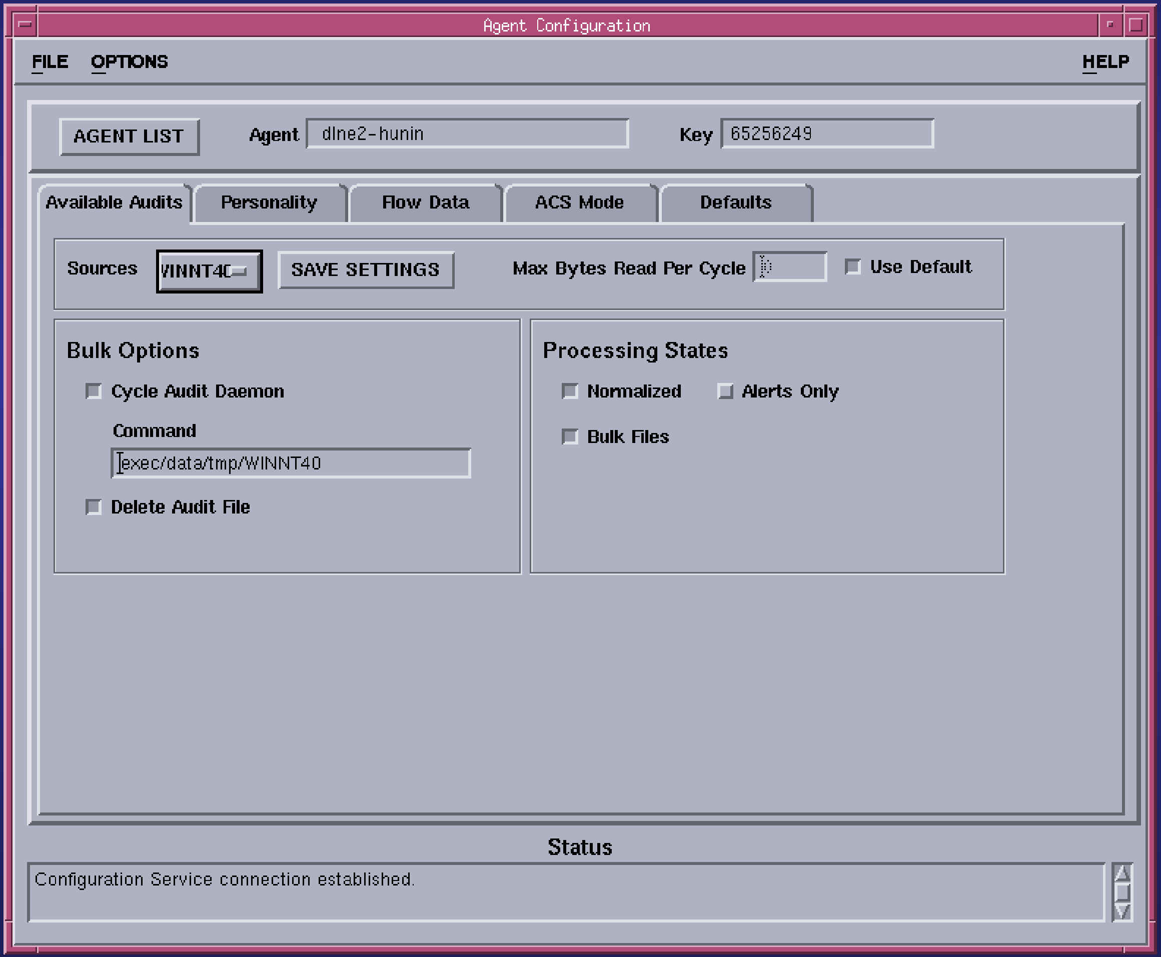
Selected Sources: XHAC

Report Name: Svr06

XHAC query being validated.

The Audit Review Tool allows for the examination of the actual native audits related to any circumstance requiring further analysis.

PRéCis User Interfaces (continued)



Agent: dlne2-hunin

Key: 65256249

Sources: WINNT40

Max Bytes Read Per Cycle: □ Use Default

Bulk Options

□ Cycle Audit Daemon

Command: exec/data/tmp/WINNT40

□ Delete Audit File

Processing States

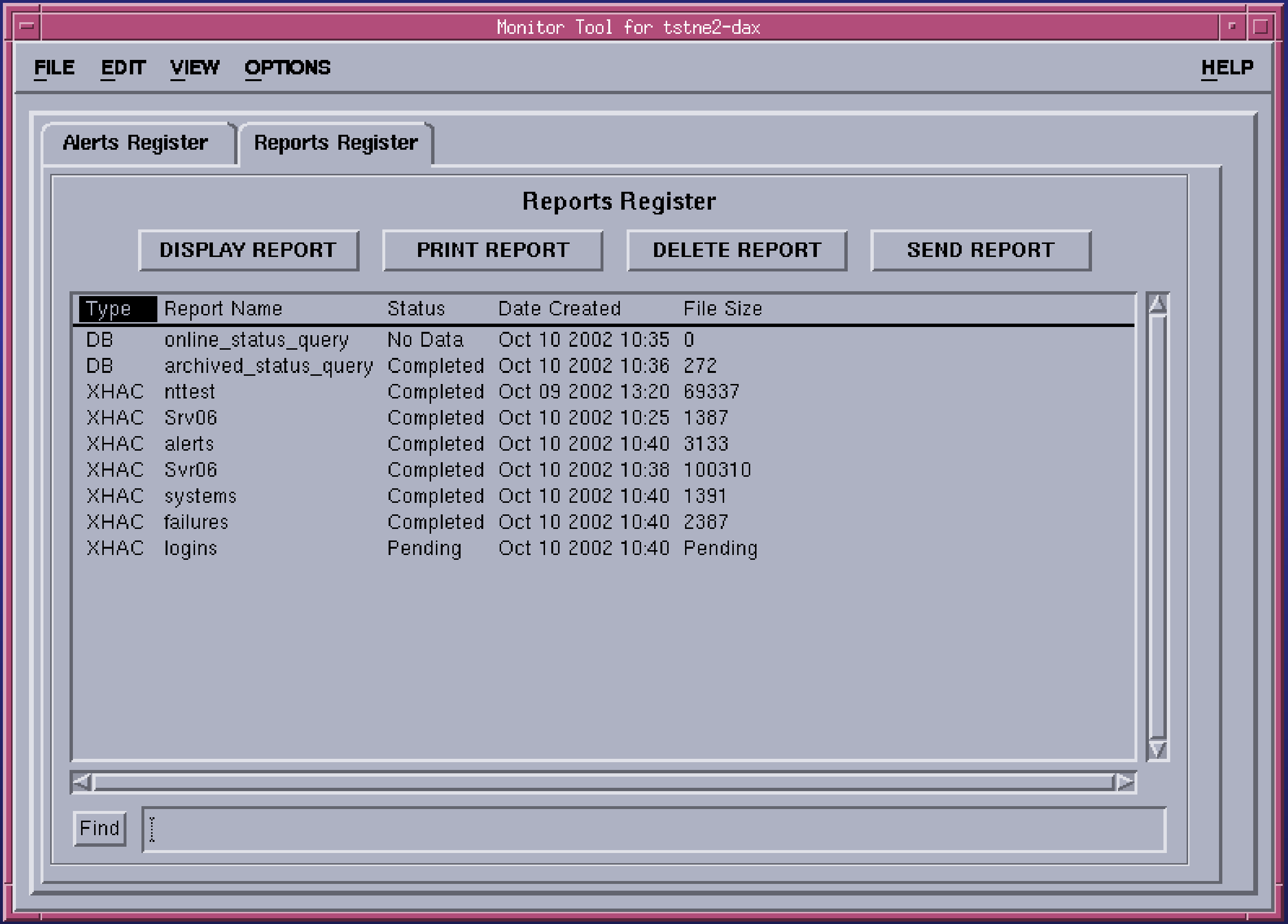
□ Normalized □ Alerts Only

□ Bulk Files

Configuration Service connection established.

The Agent Configuration Tool allows alerts to be configured based on a definable set of user actions.

PRéCis User Interfaces (continued)

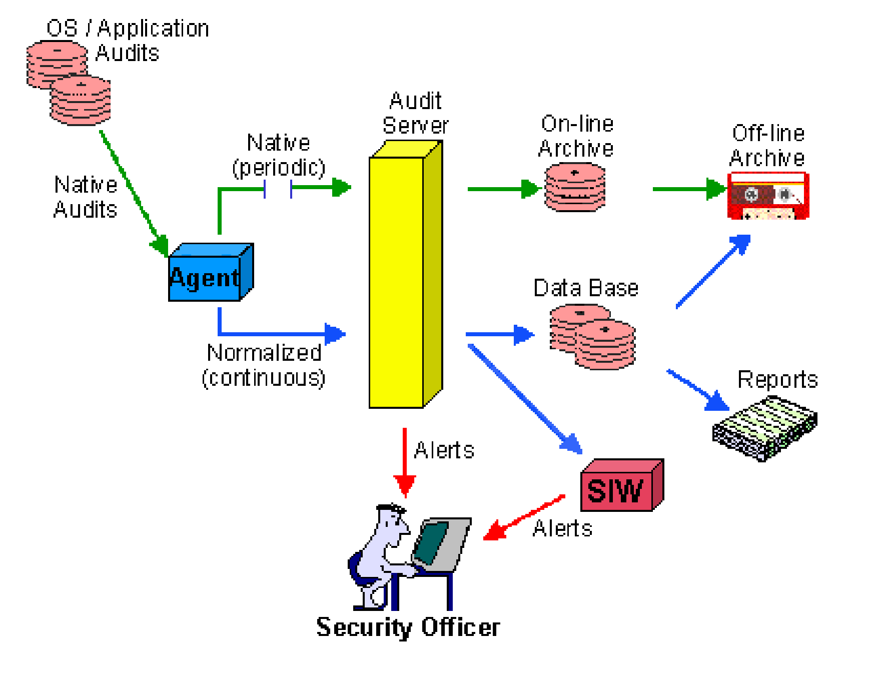


Type	Report Name	Status	Date Created	File Size
DB	online_status_query	No Data	Oct 10 2002 10:35	0
DB	archived_status_query	Completed	Oct 10 2002 10:36	272
XHAC	nttest	Completed	Oct 09 2002 13:20	69337
XHAC	Srv06	Completed	Oct 10 2002 10:25	1387
XHAC	alerts	Completed	Oct 10 2002 10:40	3133
XHAC	Svr06	Completed	Oct 10 2002 10:38	100310
XHAC	systems	Completed	Oct 10 2002 10:40	1391
XHAC	failures	Completed	Oct 10 2002 10:40	2387
XHAC	logins	Pending	Oct 10 2002 10:40	Pending

Report templates allow you to tailor reports to include headers, titles, summaries, and page breaks

Summary

- PRéCis is a distributed application that automates all aspects of processing audits on your network. It provides cradle-to-grave support for managing audit information, simplifying your day-to-day operations, yet providing the safeguards you need.
- PRéCis' real power lies in its ability to digest, analyze, and store large volumes of audits from various sources and give you concise summaries. For example, it can provide:
  - Near real-time security alerts triggered by definable user actions
  - Currently negotiating with Northrop for Windows 2003 agents



JEDI Points of Contact

Major Hans VonMilla
AFC2ISRC/INY
Infrastructure Systems Branch
(757) 225 - 1141
hans.vonmilla@langley.af.mil

Mr. Cliff Liggins
AC2ISRC/INY
JEDI Functional Manager
(202) 404 – 1160
clifford.liggins@pentagon.af.m
clifford.liggins@rl.af.mil

Capt Ryan Durante
AFRL/IFEB
JEDI Program Manager
(315) 330 - 7658
ryan.durante@rl.af.mil

Mr. Kevin Dyer
AC2ISRC/INY
JEDI Chief Engineer
(202) 404 – 1310
kevin.dyer@pentagon.af.mil
kevin.dyer@rl.af.mil

https://extranet.rl.af.mil/jedi